Subject: Unable to run OpenVPN - "openvpn --mktun --dev tap0" fails
Posted by tomfra on Thu, 18 Oct 2007 14:35:08 GMT
View Forum Message <> Reply to Message

I am trying to setup OpenVPN on one VPS using the "dummy0" trick as described at http://forum.openvz.org/index.php?t=msg&th=315 , in the wiki and some other sources.

However, when I run "openvpn --mktun --dev tap0" I get this error:

Thu Oct 18 14:04:59 2007 TUN/TAP device tap0 opened
Thu Oct 18 14:04:59 2007 Note: Cannot set tx queue length on tap0: Operation not permitted (errno=1)
Thu Oct 18 14:04:59 2007 Cannot ioctl TUNSETPERSIST(1) tap0: Operation not permitted (errno=1)
Thu Oct 18 14:04:59 2007 Exiting

/dev/tun exists. I can also create tap0 manually but that didn't help either. Both tun & bridge modules are loaded on the host.

Thanks in advance for any help

Tomas

Subject: Re: Unable to run OpenVPN - "openvpn --mktun --dev tap0" fails
Posted by maratrus on Fri, 19 Oct 2007 11:12:53 GMT
View Forum Message <> Reply to Message

Hi,

1. OpenVZ kernel prohibits to set persistent mode for tun device inside VPS.
If we allow to do this we have to remove the structures associated with device during the VPS stopping and in is not so easy.

2. You can use openvpn without persistent mode.

Thank You!

Subject: Re: Unable to run OpenVPN - "openvpn --mktun --dev tap0" fails
Posted by tomfra on Fri, 19 Oct 2007 13:04:22 GMT
View Forum Message <> Reply to Message

OK, thanks for the answer!

By the way, does someone have a step-by-step how-to on how to install OpenVPN on an OpenVZ VPS? I found something but it would be nice if there was a more complete "how-to", the instructions at openvpn.net are not overly clear...

Tomas

Subject: Re: Unable to run OpenVPN - "openvpn --mktun --dev tap0" fails
Posted by bwoo on Thu, 25 Oct 2007 19:19:20 GMT
View Forum Message <> Reply to Message

So is there a way of running OpenVPN as a server inside a VE?

Subject: Re: Unable to run OpenVPN - "openvpn --mktun --dev tap0" fails
Posted by tomfra on Thu, 25 Oct 2007 21:31:01 GMT
View Forum Message <> Reply to Message

bwoo wrote on Thu, 25 October 2007 21:19So is there a way of running OpenVPN as a server inside a VE?

Yes, it is! I've just finished installing & testing it, with some help from the Experts Exchange and a lot of Googling...

I installed it in the routing mode as the "road warrior" setup plus with routing all Internet traffic through the VPN tunnel. It works great, but the config is a bit tricky.

"openvpn --mktun --dev tap0" is not needed to make it work, also the "dummy0" trick is not needed for the routing setup, it is needed for the bridging setup which I have not tested but I am sure that it would work too.

Sometime I will hopefully write the "Howto install OpenVPN on an OpenVZ VPS" but it would be something like this (on CentOS 5):

1) Add rpmforge to your list of yum repos - simply install the correct rpm for your distro from http://dag.wieers.com/rpm/packages/rpmforge-release/

2) yum -y install openvpn

3) Install the openvpn webmin module, it is great for creating the certificates, monitoring the VPN connections etc. It's a bit tricky for configuring so you will have to play with it for a while.

4) You will need the /dev/tun device in your VPS. The how-to is at http://wiki.openvz.org/VPN_via_the_TUN/TAP_device. If you haven't done so already, do

"modprobe tun" on the hardware node, I believe it should be added into /etc/init.d as well.

5) server.conf file could roughly look something like this:

```
port 1194
tls-server
mode server
proto udp
dev tun0
ca keys/myserver/ca.crt
cert keys/myserver/defaultserverkey.crt
key keys/myserver/defaultserverkey.key
dh keys/myserver/dh2048.pem
server 10.8.0.0 255.255.255.0
push "redirect-gateway def1"
push "dhcp-option DNS 10.8.0.1"
crl-verify keys/myserver/crl.pem
cipher AES-256-CBC
user nobody
group nobody
status servers/myserver/logs/openvpn-status.log
log-append servers/myserver/logs/openvpn.log
verb 2
mute 20
max-clients 500
management 127.0.0.1 4444
keepalive 10 120
client-config-dir /etc/openvpn/servers/myserver/ccd
comp-lzo
persist-key
persist-tun
ccd-exclusive
```

The 2 occurences of "push" are needed if you want to route all Internet traffic, including web etc., through the VPN tunnel, otherwise comment them out. Make sure the certificate & other paths correspond with those valid for your server.

If you set the push "dhcp-option DNS 10.8.0.1", you will need to install Bind or other DNS server on the VPS (listening on the main VPS IP). Or you can specify any public IP of DNS servers accepting queries from the VPS IP.

6) Client side:

I installed openvpn on my Win XP Home PC as a part of the OpenVPN GUI you can get at http://openvpn.se . Rename the Virtual TAP Network Adapter to "OpenVPN" (or something else but you will need to specify the name in the dev-node switch).

client.conf example:

```
client
dev tun
pull
dev-node OpenVPN
proto udp
remote PUBLIC_IP_OF_YOUR_VPN_SERVER 1194
resolv-retry infinite
nobind
persist-key
persist-tun
ca ca.crt
cert defaultclientkey.crt
key defaultclientkey.key
ns-cert-type server
cipher AES-256-CBC
keysize 256
comp-lzo
verb 3
mute 20
```

The "dev", "proto" & "cipher" switches must be the same as on the server. My chosen cipher - "AES-256" is somewhat extreme so you may comment it out (together with the "keysize" switch and OpenVPN will then default to Blowfish).

7) On the server:

service openvpn start

This should create the tun0 device I believe. Then do:

```
/sbin/iptables -A FORWARD -j ACCEPT -p all -s 0/0 -i tun0
/sbin/iptables -A FORWARD -j ACCEPT -p all -s 0/0 -o tun0
/sbin/iptables -t nat --flush
/sbin/iptables -t nat -A POSTROUTING -s ! x.x.x.x -o venet0 -j SNAT --to-source x.x.x.x
```

Replace x.x.x.x with your VPS public IP address. You should probably include those lines in the openvpn init file in /etc/init.d . Technically, only the last line may be necessary. There are probably better ways but this should work. I use CSF firewall and I added those lines to csfpre.sh instead.

8) Now you should be able to create the VPN tunnel from the client side.

It's not a perfect how-to but at least it could give you a few hints.

Tomas

Subject: Re: Unable to run OpenVPN - "openvpn --mktun --dev tap0" fails
Posted by bwoo on Fri, 26 Oct 2007 03:15:51 GMT
View Forum Message <> Reply to Message

tomas,

Thanks for the howto! Have you been able to get bridging to work though? I've found routing seems to result in lower performance. How is your performance?

ben

Subject: Re: Unable to run OpenVPN - "openvpn --mktun --dev tap0" fails
Posted by tomfra on Fri, 26 Oct 2007 10:05:11 GMT
View Forum Message <> Reply to Message

I haven't tried the bridging setup but I believe that "snowdeal" was able to make it run - take a look at http://forum.openvz.org/index.php?t=msg&goto=1761&&srch=dummy0+openvpn#msg_1761 .

Shouldn't routing show actually better performance than bridging? That's at least how they say it on the openvpn website. I haven't tested the performance as I've been focusing on making it work and my Internet connection has been of low quality lately so it's not easy to do any speedtests etc.

Tomas

Subject: Re: Unable to run OpenVPN - "openvpn --mktun --dev tap0" fails
Posted by bwoo on Fri, 26 Oct 2007 17:46:44 GMT
View Forum Message <> Reply to Message

tomas,

I followed your howto, and I have success in connecting, but I can't get to my main network.. On my client side, it gives me:

Fri Oct 26 13:40:16 2007 route ADD 192.168.0.0 MASK 255.255.255.0 192.168.201.1
Fri Oct 26 13:40:16 2007 Warning: route gateway is not reachable on any active network adapters: 192.168.201.1
Fri Oct 26 13:40:16 2007 Route addition via IPAPI failed
Fri Oct 26 13:40:16 2007 route ADD 192.168.201.0 MASK 255.255.255.0 192.168.201.1
Fri Oct 26 13:40:16 2007 Warning: route gateway is not reachable on any active network adapters: 192.168.201.1
Fri Oct 26 13:40:16 2007 Route addition via IPAPI failed

My main network is 192.168.0.0/24
My "routed" network is 192.168.201.0/24

I tried to ping 192.168.201.1 from my client and still couldn't reach it..

I commented out the push redirect-gateway per your suggestion..

Subject: Re: Unable to run OpenVPN - "openvpn --mktun --dev tap0" fails
Posted by tomfra on Fri, 26 Oct 2007 19:11:19 GMT
View Forum Message <> Reply to Message

I am not an "OpenVPN guru", but it would be helpful if you could post the full server & client config files if they differ from the examples I posted.

If I understand it correctly - the 192.168.0.0/24 IPs are used by your "real" network adapter and the 192.168.201.0/24 subnet is used by the VPN TAP Virtual Network Adapter, right?

If it is so it looks almost as if it was all reversed. I mean, in my log the first "route ADD" record looks like this:

"route ADD VPN_PUBLIC_IP MASK 255.255.255.255 172.23.35.10"

172.23.35.10 is my "real network adapter" gateway.

Hmm... just thinking aloud but what does this line look like in your client config file:

"remote PUBLIC_IP_OF_YOUR_VPN_SERVER 1194"

Is the "PUBLIC_IP_OF_YOUR_VPN_SERVER" really a public IP in your config file?

Tomas

Subject: Re: Unable to run OpenVPN - "openvpn --mktun --dev tap0" fails

Posted by OpenVZ on Thu, 29 Nov 2007 18:33:56 GMT
View Forum Message <> Reply to Message

tomfra wrote on Thu, 25 October 2007 17:31
/sbin/iptables -A FORWARD -j ACCEPT -p all -s 0/0 -i tun0
/sbin/iptables -A FORWARD -j ACCEPT -p all -s 0/0 -o tun0
/sbin/iptables -t nat --flush
/sbin/iptables -t nat -A POSTROUTING -s ! x.x.x.x -o venet0 -j SNAT --to-source x.x.x.x

Replace x.x.x.x with your VPS public IP address. You should probably include those lines in the openvpn init file in /etc/init.d . Technically, only the last line may be necessary. There are probably better ways but this should work. I use CSF firewall and I added those lines to csfpre.sh instead.

Hello tomfra,

thank you for this HOWTO.

It works.. But only if I set a public IP to the VPS.

If I set an internal IP to VPS like 192.168.1.5, (for testing) I can use it as a webserver (=>can reach from outside), but openvpn doesn't work..

What should I do to get it working?

Thank you..

Subject: Re: Unable to run OpenVPN - "openvpn --mktun --dev tap0" fails
Posted by tomfra on Thu, 29 Nov 2007 18:44:11 GMT
View Forum Message <> Reply to Message

Instead of this line:

/sbin/iptables -t nat -A POSTROUTING -s ! x.x.x.x -o venet0 -j SNAT --to-source x.x.x.x

try this one:

/sbin/iptables -t nat -A POSTROUTING -s 10.88.0.0/16 -o venet0 -j SNAT --to-source 192.168.1.5

where 10.88.0.0/16 is the internal IP range assigned by OpenVPN, you will very likely have a different one so don't forget to change it.

I am not saying it will work, I am really not a "pro" in this field, but it may be worth a try.

Tomas

Subject: Re: Unable to run OpenVPN - "openvpn --mktun --dev tap0" fails
Posted by OpenVZ on Thu, 29 Nov 2007 19:10:05 GMT
View Forum Message <> Reply to Message

tomfra wrote on Thu, 29 November 2007 13:44Instead of this line:

/sbin/iptables -t nat -A POSTROUTING -s ! x.x.x.x -o venet0 -j SNAT --to-source x.x.x.x

try this one:

/sbin/iptables -t nat -A POSTROUTING -s 10.88.0.0/16 -o venet0 -j SNAT --to-source 192.168.1.5

where 10.88.0.0/16 is the internal IP range assigned by OpenVPN, you will very likely have a different one so don't forget to change it.

I am not saying it will work, I am really not a "pro" in this field, but it may be worth a try.

Tomas

Hello,

thank you. I did try it.. Not working.

If I look at the log, the vpn request doesn't come to the vps.. No entry about the request..

To forward port 1194 I use this command (in the hardware node):

iptables -t nat -A PREROUTING -p tcp -d 192.168.1.5 --dport 1194
 -i eth0 -j DNAT --to-destination PUBLIC_IP_OF_HARDWARE_NODE:1194

Maybe is it wrong or not enough?

Subject: Re: Unable to run OpenVPN - "openvpn --mktun --dev tap0" fails
Posted by tomfra on Thu, 29 Nov 2007 19:24:51 GMT
View Forum Message <> Reply to Message

Sorry, I can't be of more help in this case I am afraid. It's a scenario I have not tried. You may have some luck with the openvpn.net mailing list, I am sure someone had a similar problem in the

past.

Tomas

Subject: Re: Unable to run OpenVPN - "openvpn --mktun --dev tap0" fails
Posted by OpenVZ on Thu, 29 Nov 2007 19:36:07 GMT
View Forum Message <> Reply to Message

Ok, thank you..

Subject: Re: Unable to run OpenVPN - "openvpn --mktun --dev tap0" fails
Posted by stuartornum on Sun, 02 Dec 2007 10:39:46 GMT
View Forum Message <> Reply to Message

I did a HOWTO on setting up OpenVPN on OpenVZ and Xen a while ago.

Can be found at webhostingtalk.com

Direct link:

http://www.webhostingtalk.com/showthread.php?t=595436&hi ghlight=howto+openvpn

---